signing key expiry data to a plurality of clients, that are selectable on a per client basis wherein the digital signature key pairs are not shared among users;

determining whether a digital signature key pair update request has been received from a client unit;

receiving a new digital signature key pair from the client unit in response to the digital signature key pair update request; and

wherein the step of associating the stored selected expiry data includes creating a new digital signature certificate containing the selected public key expiry data selected for the client that generated the digital signature key pair update request.

4. (Delete)

14. (Six times amended): A system for providing updated digital signature key pairs to a plurality of clients in a public key system comprising:

multi-client management means for providing selectable digital signature expiry data to a plurality of clients and not by a client, including at least both public verification key expiry data and private signing key expiry data that are selectable on a per client basis wherein the digital signature key pairs are not shared among users;

means, accessible by the multi-client manager means, for digitally storing both selected public key expiry data and selected private key expiry data for association with a new digital signature key pair;

means, responsive to the stored selected public key expiry data, for associating the stored selected expiry data with the new digital signature key pair to affect a transition from an old digital signature key pair to a new digital signature key pair;

means for determining whether a digital signature key pair update request has been received from a client unit;

means for receiving a new digital signature key pair from the client unit in response to the digital signature key pair update request; and

wherein the means for associating the stored selected expiry data creates a new digital signature certificate containing the selected public key expiry data selected for the client that generated the digital signature key pair update request.

18. (Delete)

21. (Six times amended): A storage medium comprising:

a stored program for execution by a processor wherein the program facilitates providing updated digital signature key pairs in a public key system by:

allowing entry of selectable expiry data for a plurality of clients and not through a client, including both at least public verification key expiry data and signing private key expiry data that are selectable on a per client basis wherein the digital signature key pairs are not shared among users;

digitally storing both selected public key expiry data and selected private key expiry data for association with a new digital signature key pair;

associating the stored selected expiry data with the new digital signature key pair to affect a transition from an old digital signature key pair to a new digital signature key pair;

determining whether a digital signature key pair update request has been received from a client unit;

receiving a new digital signature key pair from the client unit in response to the digital signature key pair update request; and

creating a new digital signature certificate containing the selected public key expiry data selected for the client that generated the digital signature key pair update request.

24. (Delete)

30. (Six times amended): A method for providing updated digital signature key pairs to a plurality of clients in a public key system comprising the steps of:

providing, by a multi-client manager unit and not by a client, selectable digital signature expiry data including at least public verification key expiry data, and selectable private signing key expiry data to a plurality of clients, that are selectable on a per client basis wherein the digital signature key pairs are not shared among users;

digitally storing both selected public key expiry data and selected private key expiry data for association with a new digital signature key pair;

determining whether a digital signature key pair update request has been received from a client unit;

receiving a new digital signature key pair from the client unit in response to the digital signature key pair update request;

associating the stored selected expiry data with the new digital signature key pair to affect a transition from an old digital signature key pair to a new digital signature key pair; and

wherein the step of associating the stored selected expiry data includes creating a new digital signature certificate containing the selected public key expiry data selected for the client generating the digital signature key pair update request, a user public key, a user name and a signature of the multi-client manager unit.